JOURNAL OF NUMBER THEORY 12, 278–282 (1980)

Pythagoräische Tripel und Reziprozität in Galoisfeldern

KLAUS BURDE

Institut D für Math d. TU, Braunschweig, Pockelsstrasse 14, 33 Braunschweig, West Germany

Communicated by H. Zassenhaus

Received November 16, 1978

Ein "pythagoräisches Tripel" $a^2 + b^2 + c^2 = 0$; $a, b, c \in GF(p^f \equiv 1(4)$ nennen wir "quadratisch," wenn w in der Parametrisierung $a = w(u^2 - v^2)$, $b = 2wuv$, $c = w(u^2 + v^2)$; $u, v, w \in GF(p^f)$ Quadrat in $GF(p^f)$ ist. Die Elemente w, $a + ib$, $b + ic$, $c + ia$ sind zugleich Quadrate bzw. Nichtquadrate in $GF(p^f)$. Zyklisch permutierte quadratische Tripel bleiben daher quadratisch. Sind $p = a^2 + b^2$, $q = c^2 + d^2$; $a, c \equiv 1(2)$ ungerade rationale Primzahlen, die quadratische Reste voneinander sind, so sind die pythg. Tripel $a^2 + b^2 - p \equiv 0(q)$ und $c^2 + d^2 - q \equiv 0(p)$ beide quadratisch bzw. nichtquadratisch. Weiter gelten dann die Reziprozitätsbeziehungen zwischen Legendresymbolen

$$\left(\frac{b + p^{1/2}}{q}\right) = \left(\frac{d + q^{1/2}}{p}\right), \qquad \left(\frac{2(a + p^{1/2})}{q}\right) = \left(\frac{2(c + q^{1/2})}{p}\right),$$

wobei $p^{1/2}$ eine Basis des Quadrates p in $\mathbb{Z}$. ist und $q^{1/2}$ entsprechend erklärt ist.

Unter einem "rationalen pythagoräischen Tripel" versteht man drei ganz-rationale Zahlen a, b, c, die

$$a^2 + b^2 = c^2;\ a, b, c \in \mathbb{Z} \tag{1}$$

erfüllen. Diese Tripel werden bekanntlich—siehe etwa Dickson [2, Vol. II, Ch. IV]—durch

$$a = w(u^2 - v^2),\ b = 2wuv,\ c = w(u^2 + v^2); \quad u, v, w \in \mathbb{Z} \tag{2}$$

parametrisiert.

Ganz Entsprechendes gilt, wenn man den Ring $\mathbb{Z}$ der ganz-rationalen Zahlen durch ein beliebiges Galoisfeld $GF(p^f)$; $p \neq 2$ ersetzt.

SATZ 1. *Die pythagoräischen Tripel eines Galoisfeldes*

$$a^2 + b^2 = c^2; \qquad a, b, c \in GF(p^f),\ p \neq 2$$

0022-314X/80/020278–05$02.00/0

werden durch

$$a = w(u^2 - v^2),\ b = 2wuv,\ c = w(u^2 + v^2); \qquad u, v, w \in GF(p^f) \tag{3}$$

parametrisiert.

Beweis. Durch (3) sind offenbar stets (pythagoräische Tripel in $GF(p^f)$ gegeben. Sei umgekehrt a, b, c ein solches Tripel. Wegen

$$(c + a)(c - a) = c^2 - a^2 = b^2 \tag{4}$$

sind $c \pm a$ beides Quadrate bzw. Nichtquadrate in $GF(p^f)$. Wir können daher

$$c + a = 2wu^2,\ c - a = 2wv^2; \qquad u, v, w \in GF(p^f) \tag{5}$$

setzen, woraus (3) bei entsprechender Vorzeichenwahl für u, v folgt.

Die in der Form übereinstimmenden Parametrisierungen (2), (3) führen für Restklassenkörper $\mathbb{Z}_p = GF(p)$; $p \neq 2$ direkt zu dem

SATZ 2. *Die pythagoräischen Tripel modulo* $p \neq 2$

$$a^2 + b^2 = c^2; \qquad a, b, c \in \mathbb{Z}_p,\ p \neq 2$$

sind genau die Bilder modulo p der rationalen pythagoräischen Tripel.

Von dem Parameter w in (3) liegt nach (5) lediglich fest, ob es sich um ein Quadrat in $GF(p^f)$ handelt oder nicht. Genau dann, wenn w ein Quadrat ist —solche Tripel wollen wir "quadratisch" nennen—kann man diesen Faktor in (3) gleich 1 setzen bzw. weglassen. Wir definieren durch

$$\left(\frac{x}{p^f}\right) = \begin{cases} 1; & x \text{ Quadrat in } GF(p^f) \\ -1; & \text{sonst} \end{cases}, \quad x \in GF^*(p^f) \tag{6}$$

das "Legendresymbol über $GF(p^f)$."

Mit i bezeichnen wir eine primitive 4-te Einheitswurzel über $GF(p^f)$ und betrachten die beiden Fälle $i \notin GF(p^f)$—also $f = 1$ und $p \equiv 3(4)$—und $i \in GF(p^f)$—also $p^f \equiv 1(4)$—getrennt.

SATZ 3. *Von den beiden pythagoräischen Tripeln modulo* $p \equiv 3(4)$

$$a^2 + b^2 = c^2,\ b^2 + a^2 = c^2; \qquad a, b, c \in \mathbb{Z}_p,\ p \equiv 3(4)$$

ist genau eins quadratisch.

Beweis. Bei der Parametrisierung (3) gilt neben (4), (5) auch

$$(c + b)(c - b) = c^2 - b^2 = a^2 \tag{4'}$$

$$c + b = w(u + v)^2. \tag{5'}$$

Mit $(2/p) = -1$; $p \equiv 3(4)$ hat man daher

$$\left(\frac{w}{p}\right) = \left(\frac{c \pm b}{p}\right) = -\left(\frac{c \pm a}{p}\right); \qquad p \equiv 3\ (4),$$

woraus Satz 3 folgt.

Im Fall $i \in GF(p^f)$ können wir—durch Übergang von c zu ic—zu "symmetrischen pythagoräischen Tripeln"

$$a^2 + b^2 + c^2 = 0; \qquad a, b, c, i \in GF(p^f) \tag{7}$$

mit der Parametrisierung

$$a = w(u^2 - v^2),\ b = 2wuv,\ c = iw(u^2 + v^2); \qquad u, v, w, i \in GF(p^f) \tag{8}$$

übergehen.

SATZ 4. *Für ein symmetrisches pythagoräisches Tripel* (7) *mit der Parametrisierung* (8) *gilt*

$$\left(\frac{a \pm ib}{p^f}\right) = \left(\frac{b \pm ic}{p^f}\right) = \left(\frac{c \pm ia}{p^f}\right) = \left(\frac{w}{p^f}\right). \tag{9}$$

Die Eigenschaft eines solchen Tripels, quadratisch zu sein, ist daher invariant gegenüber zyklischer Vertauchung von a, b, c und invariant gegenüber allen Permutationen von a, b, c genau für $(i/p^f) = 1$, *d.h.* $p^f \equiv 1(8)$.

Beweis. Die Unabhängigkeit der Symbole in (9) von dem im "Zähler" gewählten Vorzeichen ergibt sich für das erste Symbol aus

$$(a + ib)(a - ib) = a^2 + b^2 = (ic)^2,$$

und entsprechend für die anderen Symbole. Die weitere Aussage des Satzes folgt dann aus

$$\begin{aligned} a + ib &= w(u^2 - v^2 + 2iuv) &&= w(u + iv)^2, \\ b + ic &= w(2uv - u^2 - v^2) &&= w(iu - iv)^2, \\ c + ia &= w(2iu^2) &&= w((1 + i)u)^2. \end{aligned}$$

Nun seien $p, q \equiv 1(4)$ rationale Primzahlen, die quadratische Reste voneinander sind

$$(p/q) = (q/p) = 1; \qquad p, q \equiv 1(4) \tag{10}$$

und[1]

$$\begin{aligned} p &= \pi\bar{\pi}; \qquad \pi = a + ib \in \mathbb{Z}[i], \quad a, c \equiv 1\ (2); \\ q &= \chi\bar{\chi}; \qquad \chi = c + id \in \mathbb{Z}[i], \quad b, d \equiv 0\ (2); \end{aligned} \tag{11}$$

ihre Zerlegungen im Gaußschen Zahlring. Dann sind

$$a^2 + b^2 = p, \qquad c^2 + d^2 = q \tag{12}$$

—modulo q bzw. p betrachtet—pythagoräische Tripel in $\mathbb{Z}_q$ bzw. $\mathbb{Z}_p$. Die entsprechenden summetrischen Tripel

$$\begin{aligned} a^2 + b^2 + (ip^{1/2})^2 = 0,\ c^2 + d^2 + (iq^{1/2})^2 = 0; \\ a, b, i, p^{1/2} \in \mathbb{Z}_q\ ;\ c, d, i, q^{1/2} \in \mathbb{Z}_p \end{aligned} \tag{12'}$$

nennen wir die "durch p bzw. q induzierten pythagoräischen Tripel in $\mathbb{Z}_q$ bzw. $\mathbb{Z}_p$."

Nach dem komplexen quadratischen Reziprozitätsgesetz gilt—siehe hierzu etwa Burde [1]—

$$\left(\frac{a \pm ib}{q}\right) = \left(\frac{\pi}{\chi}\right) = \left(\frac{\chi}{\pi}\right) = \left(\frac{c \pm id}{p}\right), \tag{13}$$

wobei die mittleren Symbole die komplexen quadratischen Restsymbole modulo χ bzw. π sind.

Aus (13) erhält man mit Satz 4, genauer (9)—angewandt auf (12')—zwei weitere Reziprozitätsformeln für Legendresymbole.

SATZ 5. *Sind $p = a^2 + b^2$, $q = c^2 + d^2$; $a, c \equiv 1(2)$[1] ungerade rationale Primzahlen, die quadratische Reste voneinander sind, so gelten die Reziprozitäten*[2]

$$\left(\frac{b \pm p^{1/2}}{q}\right) = \left(\frac{d \pm q^{1/2}}{p}\right); \qquad a, b, i, p^{1/2} \in \mathbb{Z}_q\,, \tag{14}$$

$$\left(\frac{i(a \pm p^{1/2})}{q}\right) = \left(\frac{i(c \pm q^{1/2})}{p}\right); \qquad c, d, i, q^{1/2} \in \mathbb{Z}_p\,. \tag{15}$$

[1] Wegen (10) braucht man in (11) nur die angegebene schwache Normierung der Primfaktoren. Für $p^f \equiv 1(8)$ wird auch diese überflüssig.

[2] Wegen $2i = (1 + i)^2$ kann man (15) auch in der Form (15') $(2(a \pm p^{1/2})/q) = (2(c \pm q^{1/2})/p)$ schreiben.

Für pythagoräische Tripel folgt aus (13) mit Satz 4 das "Reziprozitätsgesetz":

SATZ 6. *Sind* $p, q \equiv 1(4)$ *rationale Primzahlen, die quadratische Reste voneinander sind, so sind die von ihnen induzierten pythagoräischen Tripel in* Z_q *bzw.* Z_p *entweder beide quadratisch oder beide nicht-quadratisch.*

Satz 6 drückt eine recht partielle Reziprozitätseigenschaft pythagoräische Tripel aus, hinter der man eine allgemeinere Reziprozitätsbeziehung zwischen pythagoräischen Tripeln in Galoisfeldern vermuten möchte. Es wäre nicht uninteressant, die Form einer solchen allgemeineren Beziehung und insbesondere die zu ihr äquivalenten Reziprozitäten zwischen quadratischen Resten aufzufinden.

LITERATUR

1. K. BURDE, Zur Herleitung von Reziprozitätsgesetzen unter Benutzung endlicher Körper, *J. Reine Angew. Math.* **293/294** (1977), 418–427.
2. L. E. DICKSON, "History of the Theory of Numbers," Chelsea, Washington, 1919.

Printed in Belgium